STATE OF ALABAMA

Information Technology Standard

Standard 650-01S2: Access Management

1. INTRODUCTION:

It is the policy of the State to control unauthorized access in order to protect the state resources and to maintain the safest possible environment for employees and visitors. This is accomplished, in part, by the use of network controlled and monitored access points. Access into many buildings, offices, and parking areas on the Capitol campus is controlled by a centrally administered access management system. The Capitol Complex Security Systems office is responsible for the issuance of access cards used with this system and programming parameters to lock/unlock controlled access points.

2. OBJECTIVE:

Ensure all authorized access card holders comply with the requirements of access card issuance and use.

3. SCOPE:

These requirements are applicable to all State employees and contractors who are issued an access card, to all access card coordinators, and to the heads of agencies utilizing the access card system.

4. REQUIREMENTS:

4.1 GENERAL

Access cards are issued to State employees and contractors requiring after-hours access, access to facilities that are locked 24/7, or access to certain gated parking areas. Personnel not requiring an access card for access will instead be issued a photo ID card.

Access cards and ID cards are State property and are subject to the rules of use as determined by the issuing authority, as stated in this document, and any additional agency requirements.

Personnel requiring an access card or ID card shall complete a "Request for Access Card Authorization Form" and obtain agency Director or Access Card Coordinator authorization. The form must be completed before an access card or ID card will be issued.

Access cards and ID cards issued by the Department of Finance require a current photo. Photos shall be taken at the Capitol Complex Security Systems office.

Access cards are individually assigned and are authorized for use by the card holder only. Access cards are not transferable and until returned are the responsibility of the person to whom issued. If a card holder lends their card to another individual, access card privileges may be suspended or revoked.

4.2 RESPONSIBILITIES

4.2.1 Agency Head

Assign an Access Card Coordinator. Each agency within the Capitol Complex that utilizes the cardkey access system must appoint an Access Card Coordinator.

4.2.2 Access Card Coordinator

The Access Card Coordinator serves as the contact person for their agency for the issuance of access cards and is responsible for authorizing access, revoking privileges when necessary, collecting access card from departing card holders, and returning access cards to the Security Systems Office, Folsom Building, Suite 121 (agencies will continue to be billed as applicable until access cards are turned in).

4.2.3 Card Holder

Turn in access cards and ID cards to the agency Access Card Coordinator upon departure (inter-agency transfer, retirement, resignation, termination, loss of parking space, end of contract, etc.), if the card fails to work properly, or if it becomes damaged (cracked or broken).

Maintain accountability for the access card at all times; protect from loss, theft, or damage. . If an access card or ID card is lost, notify the agency Access Card Coordinator immediately, or after-hours notify the Capitol Complex Security Systems Administrator at 242-0915.

Card holders shall be responsible for paying a $10.00 access card replacement fee.

5. DEFINITIONS:

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 650-01: Physical Security

6.2 RELATED DOCUMENTS

Information Technology Standard 650-01S1: Physical Security

Signed by Eugene J. Akers, Ph.D., Assistant Director

Revision History

Version	Release Date	Comments
Original	07/14/2006	